Claims

What is claimed is:

1. A method for updating an on-board clock device to compensate for individual deviation from a time value comprising the steps of:
a) providing a signal from each of a plurality of modules indicating a time associated with said module and for use by said module in performing time stamping operations;
b) receiving the signal from each of the plurality of modules and determining a synchronization between the modules to detect synchronized modules and modules that are other than synchronized with the synchronized modules; and,
c) when a module is detected as other than synchronized with the synchronized modules, automatically performing one of synchronizing that module with the synchronized modules and disabling that module from performing timestamping operations.

2. A method according to claim 1 wherein each module of the plurality of modules is inserted within a same module housing for at least a same overlapping period of time, the module housing electrically connected to a computer system and for providing communication between each module of the plurality of modules and between the plurality of modules and the computer system.

3. A method according to claim 2 comprising the additional step prior to step (c) of:
authenticating each module of the plurality of modules to determine at least a unique module identification and a current initialization status of said module; and
wherein only those modules that are authenticated are evaluated for synchronization.

4. A method according to claim 3 wherein the step of performing one of synchronizing that module and disabling that module comprises a step of disabling a module that is other than synchronized with the synchronized modules by erasing the cipher data stored within that module and relating to timestamping.

5. A method according to claim 4 wherein the step of performing one of synchronizing that module and disabling that module comprises a step of disabling a module that is other than synchronized with the synchronized modules by erasing all the cipher data stored within that module.

6. A method according to claim 3 wherein the step of performing one of synchronizing that module and disabling that module comprises a step of disabling a module that is other than synchronized with the synchronized modules by setting a flag within the module that is other than synchronized with the synchronized modules, the flag for preventing operation of the module for timestamping operations.

7. A method according to claim 6 wherein the flag is for preventing operation of the module for all secuirty operations.

8. A method according to claim 3 wherein the step of performing one of synchronizing that module and disabling that module comprises a step of synchronizing that module that is other than synchronized with the synchronized modules including the steps of:
initializing the detected module;
sending a new value characteristic of a current time of day to said module; and,
setting the real time clock of said module in dependence upon the received new value.

9. A method according to claim 3 wherein a predetermined first module of the plurality of modules is a master module for performing processor functions for periodically verifying synchronization of each module of the plurality of modules.

10. A method according to claim 9 wherein the signal from each module of the plurality of modules includes at least data for the authentication of said module and data indicating real time information associated with said module.

11. A method according to claim 10 wherein the signal from each of the plurality of modules includes a first signal for providing digital data for the authentication of said

module and a second other signal for providing real time information associated with the time of transmission of the first signal.

12. A method according to claim 11 wherein the first signal for providing digital data for the authentication of said module includes at least a data packet encrypted with a key for uniquely authenticating said module.

13. A method according to claim 10 wherein the signal from each of the plurality of modules includes a timestamp indicative of both the real time associated with said module and the module identifier.

14. A method according to claim 13 wherein the signal from each of the plurality of modules is provided automatically at predetermined intervals.

15. A method according to claim 14 wherein the digital data that is encrypted by each of the plurality of modules is one of a predetermined data packet stored in memory of that module and a digital document provided previously to that module from the computer system.

16. A method according to claim 13 wherein the signal from each of the plurality of modules is provided in dependence upon receiving a polling request from the master module.

17. A method according to claim 16 wherein the polling request from the master module includes the digital data for encryption by each module of the plurality of modules.

18. A method according to claim 1 comprising the steps of:
retrieving data indicative of past synchronization status for a detected module;
disabling the detected module when past synchronization status are indicative of a device reliability below a predetermined threshold; and,

synchronizing the detected module when past synchronization status are indicative of a device reliability above a predetermined threshold.

19. A method for verifying an on-board clock device to compensate for individual deviation comprising the steps of:

a) receiving a signal including a plurality of time synchronization values at each of a plurality of modules; and

b) each module determining a synchronization status of itself and, upon determining a status other than in synchronization with the other modules, disabling itself.

20. A method according to claim 19 wherein prior to step (a) each module performs the additional step of providing a value representative of a time associated with that module to each other module of the plurality of modules.

21. A method according to claim 20 wherein the signal including a plurality of time synchronization values received at each module includes a tally of modules that are synchronized with that module and a tally of modules that are other than synchronized to that module, said tallies used by each module to determine its synchronization status.

22. A method according to claim 21 wherein each module determines its synchronization status in dependence upon receiving data indicative of a predetermined minimum fraction of modules being in synchronisation therewith.

23. A method for inserting a new time stamping cryptographic module within an existing cryptographic system comprising the steps of:

a) installing a module within a communication bus;

b) detecting the module; and

c) synchronizing the module by setting the real time clock of the module in dependence upon a value indicative of a current time from the real time clocks of other modules, wherein the step of detecting the module is performed in response to the module providing a signal indicative of a non-synchronized status of the module.

24. A method for inserting a new time stamping cryptographic module within an existing cryptographic system according to claim 23 wherein the signal is provided when the module is initialized.

25. A method for inserting a new time stamping cryptographic module within an existing cryptographic system according to claim 24 wherein the step of installing the module includes the steps of:
mating a secure port of the module with a corresponding port of the communication bus;
establishing electrical communication between the module and another module;
initializing the module; and,
authenticating the module.

26. A time stamping cryptographic module comprising:
a real time clock for providing a time measurement for time stamping functions;
a microprocessor connected to the real time clock for handling at least a processing function for periodically updating the real time clock;
a secure port in electrical communication with the microprocessor for exchanging information with a device external to the module,
wherein the secure port is for mating with a corresponding port of a secure communication bus to provide a secure communication channel for exchanging a value which is characteristic of a time of day with a second other module mated with a second other corresponding port of a same secure communication bus for at least a same overlapping period of time; and,
a lock for enabling the module in a first state and for disabling the module in a second other state.

27. The apparatus according to claim 26 further comprising an on-board power source for maintaining at least an initialization status and a real time clock value characteristic of a time of day.

28. The apparatus according to claim 27 further comprising a tamper detection circuit for detecting unauthorized tampering attempts, for providing a signal in dependence thereon and for deactivating the module in response to the signal indicative of an unauthorized tampering attempt.

29. A time stamping cryptographic module comprising:
a real time clock for providing a time measurement for time stamping functions;
a microprocessor connected to the real time clock for handling at least a processing function for periodically updating the real time clock;
a secure port in electrical communication with the microprocessor for exchanging information with a device external to the module,
wherein the secure port is for mating with a corresponding port of a secure communication bus to provide a secure communication channel for exchanging a value which is characteristic of a time of day with a second other module mated with a second other corresponding port of a same secure communication bus for at least a same overlapping period of time;
means for setting a time of the real time clock in dependence upon a secured time value received from a second other module; and
a tamper detection circuit for detecting unauthorized tampering attempts and for providing a signal in dependence thereon and for deactivating the module in response to the signal indicative of an unauthorized tampering attempt.

30. The apparatus according to claim 29 further comprising an on-board power source for maintaining at least an initialization status and a real time clock value characteristic of a time of day during a power failure.